REMARKS

The Applicants and the undersigned thank Examiner Son for his careful review of this application. After entry of this Amendment, Claims 1-59 are pending in the present application, with Claims 1, 16, 27, 34, and 49 being independent. Applicants have amended Claims 1, 16, 27, 28, 34, and 49 herein. Furthermore, Applicants have amended the detailed description section of the specification to correct a typographical error. The Applicants believe that no new matter has been added to this application.

Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks

Summary of Telephonic Interview of February 17, 2005

The Applicants and the undersigned thank the Examiner for his time and consideration given during the telephonic interview of February 17, 2005. During this telephonic interview, proposed amendments to the claims were discussed. The Applicants provided the proposed amendments to the claims in advance of the interview.

Specifically, the Applicants discussed the proposed amendments to independent Claims 1 and 16, and noted that the amended claims are not taught by the prior art references cited by the Examiner. (U.S. Patent No. 6,453,345 B2 issued in the name of Trcka et al.; hereinafter the "Trcka" reference). The prior art does not describe or teach multiple alerts from multiple security devices nor does the prior art teach scope criteria that has variables that can be adjusted for analyzing security event data. Examiner Son considered the Applicants' proposed amendments and indicated that an updated search would be required for the amended claims.

The Applicants and the undersigned request the Examiner to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04, p. 700-202. Consideration and approval of this interview summary record are respectfully requested.

Amendment to the Specification

Applicants have amended a paragraph on page 11, lines 17-29 in the detailed description section of the specification to correct a typographical error. It is believed that no new matter has been added.

Claim Rejections

In the Office Action dated October 21, 2004, the Examiner rejected Claims 1-59 under 35 U.S.C. § 103(a) as being obvious over the Trcka reference, U.S. Patent No. 6,453,345 B2.

The Applicants respectfully offers remarks to traverse these rejections. The Applicants will address each independent laim separately as the Applicants believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Trcka reference fails to describe, teach, or suggest the combination of: (1) generating a plurality of alerts with a plurality of security devices at a first location; (2) creating scope criteria by adjusting variables operable for analyzing security event data, the security event data comprising the plurality of alerts; (3) collecting the security event data generated by the plurality of security devices located at a the first location; (4) storing the collected security event data at a second location; and (5) analyzing the collected security event data with the scope criteria to produce result data, the result data accessible by a plurality of clients, as recited in amended independent Claim 1.

The Trcka Reference

The Trcka reference describes a network security and surveillance system that passively generates an archival recording of raw, bi-directional computer traffic that is present on a computer network 30 as illustrated in Figure 1 of the reference. The Trcka system includes a monitoring computer 34 that is connected to the computer network 30 at a network monitoring point 36. See Figure 1 of the Trcka system reproduced below.

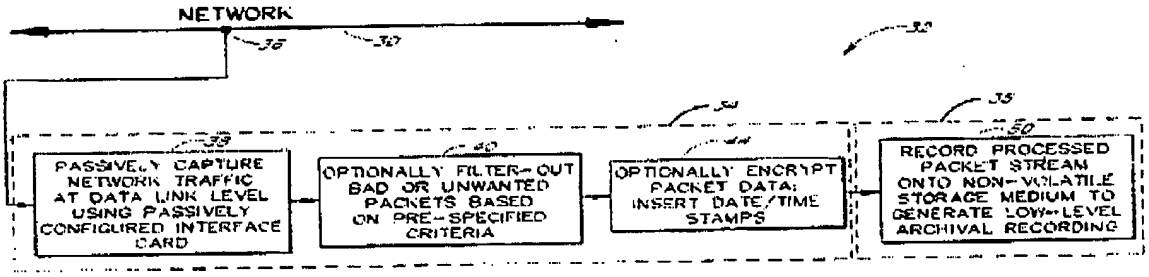

FIG. 1

The monitoring computer 34 of the Trcka reference includes an interface card 38 for passively capturing the network traffic at the data link level. The monitoring computer 34 employs a filter 40 to remove bad or unwanted packets based on pre-specified criteria. After bad or unwanted packets are removed, the computer 34 has an encryption device 44 that can encrypt the packet data as well as insert date and time stamps.

Once data and time stamps have been inserted, the computer 34 has a non-volatile storage medium 50 that can maintain a complete replica of all valid network traffic. See the Trcka reference, column 5, lines 25-45; column 6, lines 40-68; and in column 7, lines 14-42.

The Examiner admits that the Trcka reference fails to teach more than one security device collecting security event data in the network. Therefore, the Trcka reference describes a system that is opposite to a network security system that is operative for generating a plurality of alerts with a plurality of security devices at a first location.

Furthermore, the Trcka reference fails to teach creating scope criteria by adjusting variables operable for analyzing security event data, the security event data comprising the plurality of alerts, as recited in amended independent Claim 1.

Summary for Analysis of Independent Claim 1 Rejection

In light of the differences between amended independent Claim 1 and the Trcka reference, one of ordinary skill in the art recognizes that the implementations not taught by Trcka reference cannot render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 16

The rejection of Claim 16 is respectfully traversed. It is respectfully submitted that the Trcka reference fails to describe, teach, or suggest the combination of: (1) generating a plurality of alerts with the plurality of security devices at a first location; (2) creating scope criteria by adjusting variables operable for filtering security event data, the security event data comprising the plurality of alerts; (3) collecting security event data at a second location; and (4) applying the scope criteria to the security event data at a third location to produce a result, the result accessible by a plurality of clients coupled to a server, as recited in amended independent Claim 16.

Similar to the analysis of independent Claim 1, the Trcka reference fails to address generating a plurality of alerts with the plurality of security devices at a first location. Furthermore, the Trcka reference fails to teach creating scope criteria by adjusting variables operable for filtering security event data, the security event data comprising the plurality of alerts, as recited in amended independent Claim 16.

In light of the differences between amended independent Claim 16 and the Trcka reference, one of ordinary skill in the art recognizes that the Trcka reference cannot render obvious the recitations as set forth in amended independent Claim 16. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 27

The rejection of Claim 27 is respectfully traversed. It is respectfully submitted that the Trcka reference fails to describe, teach, or suggest a system that includes: (1) a plurality of security devices operable for generating security event data comprising a plurality of alerts; (2) an event manager coupled to the security devices, the event manager operable for collecting security event data from the security devices and analyzing the security event data with scope criteria comprising a plurality of defineable variables operable for analyzing the security event data; and (3) a client coupled to the event manager operable to perform an action in response to

receiving analyzed security event data from the event manager, as recited in amended independent Claim 27.

Similar to the analysis of independent Claim 1, the Trcka reference fails to address a plurality of security devices operable for generating security event data comprising a plurality of alerts. Furthermore, the Trcka reference fails to teach the implementation of an event manager operable for collecting security event data from the security devices and analyzing the security event data with scope criteria comprising a plurality of defineable variables operable for analyzing the security event data, as recited in amended independent Claim 27.

In light of the differences between amended independent Claim 27 and the Trcka reference, one of ordinary skill in the art recognizes that Trcka reference cannot render obvious the recitations as set forth in amended independent Claim 27. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 34

The rejection of Claim 34 is respectfully traversed. It is respectfully submitted that the Trcka reference fails to describe, teach, or suggest the combination of: (1) generating a plurality of alerts with a plurality of security devices at a first location; (2) creating scope criteria by adjusting variables operable for analyzing security event data, the security event data comprising the plurality of alerts; (3) collecting the security event data at a second location; (4) analyzing the collected security event data with the scope criteria at a third location to produce result data, the result data accessible by a plurality of clients; and (5) rendering the result data, in a manageable format for the plurality of clients, as recited in amended independent Claim 34.

Similar to the analysis of independent Claim 1, the Trcka reference fails to address the generating a plurality of alerts with a plurality of security devices at a first location. Furthermore, the Trcka reference fails to teach the implementation of creating scope criteria by adjusting variables operable for analyzing security event data, the security event data comprising the plurality of alerts, as recited in amended independent Claim 34.

In light of the differences between amended independent Claim 34 and the Trcka reference, one of ordinary skill in the art recognizes that the Trcka reference cannot render

obvious the recitations as set forth in amended independent Claim 34. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 49

The rejection of Claim 49 is respectfully traversed. It is respectfully submitted that the Trcka reference fails to describe, teach, or suggest the combination of: (1) generating security event data with a plurality of security devices, the security event data comprising a plurality of alerts; (2) transferring the security event data for storage in a database; (3) applying a scope criteria comprising a plurality of defineable variables to the security event data for analyzing the security event data to produce a result; and (4) accessing the result with one or more clients coupled to an application server, as recited in amended independent Claim 49.

Similar to the analysis of independent Claim 1, the Trcka reference fails to address the generating security event data with a plurality of security devices, the security event data comprising a plurality of alerts. Furthermore, the Trcka reference fails to teach the implementation of applying a scope criteria comprising a plurality of defineable variables to the security event data for analyzing the security event data to produce a result, as recited in amended independent Claim 49.

In light of the differences between amended independent Claim 49 and the Trcka reference, one of ordinary skill in the art recognizes that the Trcka reference cannot render obvious the recitations as set forth in amended independent Claim 49. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-15, 17-26, 28-33, 35-48, and 50-59

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which the depend are patentable over the cited prior art reference. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 2-15, 17-26, 28-33, 35-48, and 50-59.

CONCLUSION

Applicants submit the foregoing as a full and complete response to the Non-Final Office Action dated October 21, 2004. The Applicants and the undersigned thank Examiner Son for consideration of these remarks. Applicants submit that this Amendment places the application in condition for allowance and respectfully request such action.

If any issues exist that can be resolved with an Examiner's Amendment or a telephone conference, please contact the undersigned at 404.572.2884.

Respectfully submitted,

Steven P. Wigmore
Reg. No. 40,447

KING & SPALDING LLP
191 Peachtree Street, 45th Floor
Atlanta, Georgia 30303-1763
(404) 572-4600
K&S Docket: 05456.105005